Microsoft Exchange Server

# Exchange 2000 Outlook Web Access

White Paper

December 12, 1999

# Table of Contents


Table of Contents ..... 1

Introduction ..... 1

Features and Limitations ..... 1
- Client Support ..... 3

Architecture ..... 4
- Accessing a Server ..... 4
- WebDAV ..... 6

Usage Scenarios ..... 7
- Light Messaging ..... 7
- Roving User Support ..... 7
- Kiosks ..... 8
- Migration ..... 8

Planning Considerations ..... 8
- Network Security ..... 8
- Authentication ..... 10
  - Method 1 – Basic ..... 11
  - Method 2 – Integrated Windows ..... 11
  - Method 3 – Digest ..... 11
  - Method 4 – Anonymous Access ..... 12
  - Method 5 – Basic over SSL ..... 12
  - Additional Information on SSL ..... 12
  - Front-End and Back-End Authentication ..... 13
- Capacity Planning ..... 13
- Load Balancing ..... 14

Installation and Administration ..... 14
- Setup ..... 15
- Server Configuration ..... 15
- Outlook Web Access User management ..... 16
- Virtual Servers and Directories ..... 16
- Multilanguage Support ..... 17
  - Configuring Multilanguage support ..... 17

Migration Issues ..... 18

# Exchange 2000 Outlook Web Access

White Paper

Published: January 2000

For the latest information, please see http://www.microsoft.com/exchange/

## Introduction

Microsoft® has invested quite heavily in Web technology and the implementation of that technology into all product lines. Microsoft Exchange 2000 Server marks another step in this journey by extending back-end and client applications to support the latest advances in Web technology.
Microsoft Outlook Web Access is a tightly integrated component of Exchange 2000 and a direct descendant of Outlook Web Access introduced in Microsoft Exchange Server version 5.0. Enhancements to the Exchange 2000 architecture dramatically affect the way Outlook Web Access works. These enhancements significantly increased scalability and functionality.
This paper addresses Outlook Web Access in Exchange 2000, specifically Outlook Web Access architecture and deployment.

## Features and Limitations

Exchange 2000 contains a newly-designed version of Outlook Web Access for increased performance and scalability. Client performance and functionality are greatly improved. Exchange 2000 includes the following new features:

- *Support for Microsoft Internet Explorer 5*. When accessed through Internet Explorer 5, Outlook Web Access closely resembles the full client interface. Outlook Web Access is also more efficient for Internet Explorer 5 users because it does not require communication to the Outlook Web Access server for every mouse click in the interface, as it does with other clients.

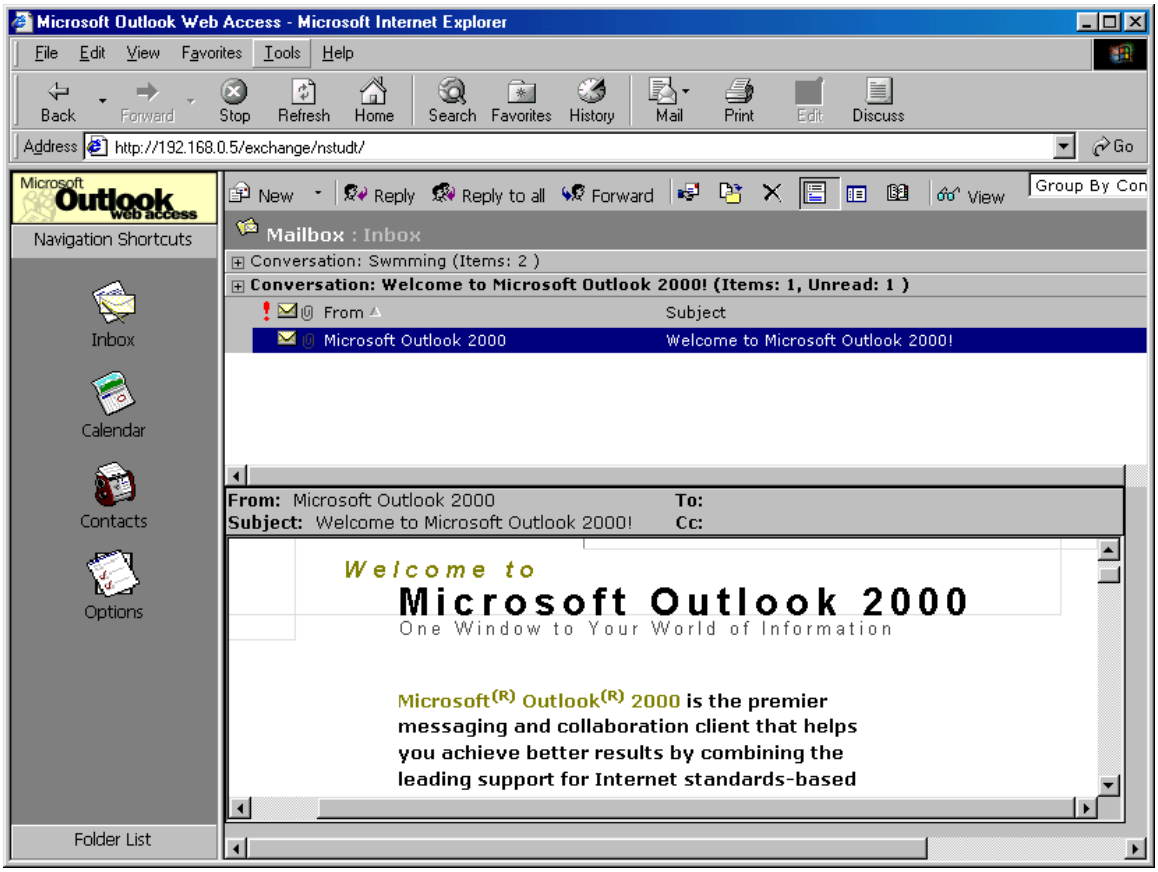

Microsoft Outlook Web Access - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address http://192.168.0.5/exchange/nstudt/
Go
Microsoft Outlook web access
Navigation Shortcuts
Inbox
Calendar
Contacts
Options
Folder List
New Reply Reply to all Forward View
Group By Con
Mailbox : Inbox
Conversation: Swmming (Items: 2 )
Conversation: Welcome to Microsoft Outlook 2000! (Items: 1, Unread: 1 )
From
Subject
Microsoft Outlook 2000
Welcome to Microsoft Outlook 2000!
From: Microsoft Outlook 2000
To:
Subject: Welcome to Microsoft Outlook 2000!
Cc:
Welcome to
Microsoft Outlook 2000
One Window to Your World of Information
Microsoft(R) Outlook(R) 2000 is the premier messaging and collaboration client that helps you achieve better results by combining the leading support for Internet standards-based

**Figure 1: Outlook Web Access Using Internet Explorer 5**

- *Support for embedded items.* Outlook Web Access now supports embedded items such as messages, appointments, and meeting requests, as well as contacts and posts.
- *Support for public folders that contain contact and calendar items.*
- *Support for named URLs referencing items.* Although previous versions of Outlook Web Access used globally unique identifiers (GUIDs) to reference items in the Information Store, items (messages, folders, and so on) are now accessed by using a plain text address such as http://server/exchange/mailbox/inbox.
- *Support for multimedia messages.* Outlook Web Access enables you to easily add audio and video clips directly into a message and send it.

Outlook Web Access is not intended to replace for Microsoft Outlook® 2000. Rather, it provides rich messaging at a lower cost in terms of network and owner overhead. Outlook Web Access includes a good deal of functionality in terms of basic messaging components such as e-mail, calendaring, and contacts.
The following table provides a quick feature comparison between Outlook Web Access and the full Outlook 2000 client.

| *Feature* | *Outlook 2000* | *Outlook Web Access (Internet Explorer 5)* | *Outlook Web Access 5.5* |
|---|---|---|---|

| **Basic features** | | | |
|---|---|---|---|
| E-mail | Yes | Yes | Yes |
| Calendaring | Yes | Yes | Yes |
| Contacts | Yes | Yes | Yes |
| Tasks | Yes | No | No |
| Embedding | Yes | No | |
| Rich Text | Yes | Yes | Yes |
| HTML | Yes | Yes | No |
| Drag-and-Drop Editing | Yes | Yes (Internet Explorer 5 only) | No |
| Shortcut Menus (obtained by right-clicking) | Yes | Yes (Internet Explorer 5 only) | No |
| Offline Use | Yes | No | No |
| Journal | Yes | No | No |
| Printing Templates | Yes | No | No |
| Outlook Rules | Yes | No | No |
| **Advanced Features** | | | |
| Timed Delivery | Yes | No | |
| Expiration | Yes | No | |
| Spelling Checker | Yes | No | No |
| Reminders | Yes | No | ? |
| Outlook Rules | | | No |
| | | | |

## Client Support

- Internet Explorer 5. This client uses Dynamic HTML and a combination of Extensible Markup Language (XML) to provide a rich set of functions for collaborative applications through the browser. Internet Explorer 5 provides a user interface that is much closer to the full version of Outlook and includes functionality such as drag-and-drop editing between folders and a tree control to open or create new folders. When creating a message, Internet Explorer 5 users can use rich text editing features to add formatting to the text.
- Other browsers. Designed for browsers that support HTML 3.2 and JavaScript. Browsers other than Internet Explorer 5 minimize the use of client side scripting, and do not provide the same functionality as Internet Explorer 5. For example, they do not include drag-and-drop editing capability or native Kerberos authentication[1].

[1] Kerberos authentication can only be used with Internet Explorer 5 and Windows 2000.

To take full advantage of Outlook Web Access features, you should use Internet Explorer 5. Any browser that is HTTP 3.2 compliant will work, but certain features and functionality will be lost. The following table compares the browsers.

| ***Feature*** | **Internet Explorer 5** | **Other** |
|---|---|---|
| HTML Text Composition | Yes | - |
| Drag-and-Drop Editing | Yes | - |
| Preview Pane | Yes | - |
| Tree Control | Yes | - |
| | | |

Most of the functionality that is lost is a result of providing backward compatibility to browsers that do not support Dynamic HTML and XML.

# Architecture

Outlook Web Access in Exchange 2000 is substantially different from the one introduced in Exchange 5.0. Exchange 5.x Outlook Web Access used ASP pages to communicate with the Exchange server that used CDO 1.2 and MAPI. In this context, Outlook Web Access for Exchange was actually a part of Internet Information Services (IIS). The reliance on MAPI-based access to the Exchange server for accessing the mailbox store limited the effective number of people who could simultaneously use the service.
Unlike previous versions of Outlook Web Access, Outlook Web Access in Exchange 2000 does not use MAPI to communicate with the mailbox store, and ASP pages are no longer used for client access. Clients continue to access the Web Access Component through HTTP; however, the IIS server hosting the component uses the new Web Store to provide access to the user's messaging functions.

Internet Information Services receives Outlook Web Access client requests as a proxy for message traffic between a Web client and an Exchange server. Internet Information Services receives the client requests, looks at the namespace, and passes the client to the appropriate Outlook Web Access scripts registered for that URL. If the server contains the Exchange 2000 database, Outlook Web Access uses a high-speed channel to access the mailbox store. If the server is a front-end server, Outlook Web Access proxies the request to a back-end server by using HTTP.

## Accessing a Server

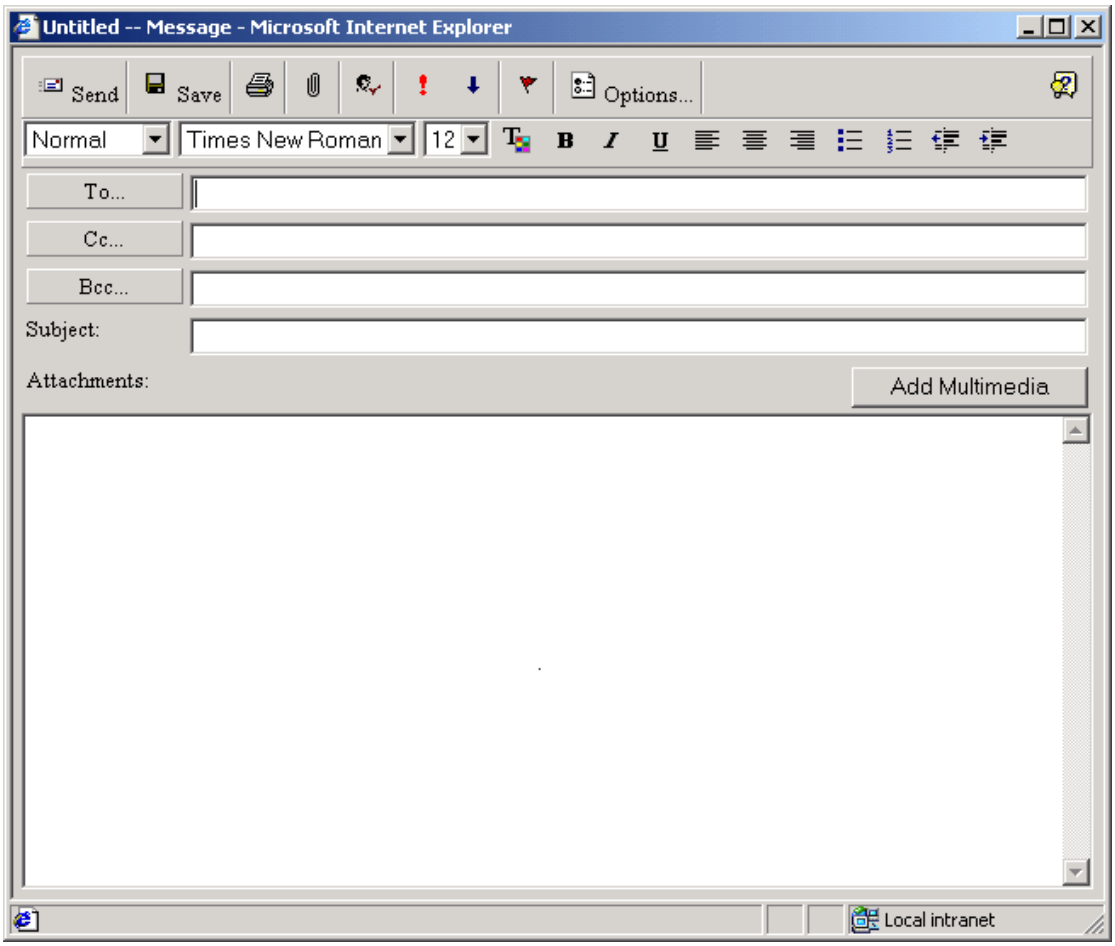
Clients direct specific requests to Outlook Web Access by using named URLs. Often the URL, such as http://owa.micrsoft.com/exchange, directs the client to the user's mailbox. Named URLs are not limited to addressing a mailbox, though. You can address most functions and components of the client by defining a specific URL.
You can open specific folders by entering the name of the folder after the mailbox name. For example, to open a calendar, type the path to the user's mailbox, then type **/calendar**, for example: http://owa.microsoft.com/exchange/*juser*/**calendar.** Likewise, you can access the Contacts folder directly by entering the path to the client's mailbox followed by **/tasks**.

Named URLs are not limited to simply accessing folders. You can open any item and perform many functions using explicit URL addressing. Many option and command verbs allow a wide range of actions:

| **Option** | **Description** |
|---|---|
| Page=x | Displays the navigation bar |
| View=*x* | Uses the Outlook view named *x* |
| Sort=*x* | Sorts by column *x* |
| Date=yyyymmdd | Displays the date in Calendar |
| Cmd=action | Performs the stated function |
| | |
| **Action** | **Description** |
| Navbar | Displays the navigation bar |
| Contents | Displays the contents of a folder |
| New | Creates a new default item in a folder |
| New&Type=x | Specifies the type of item to create |
| Options | Sets options |
| Open | Opens a message or appointment for reading |
| Edit | Opens a message or appointment for editing |
| Reply, ReplyAll, Forward | Performs message operations |
| Accept, Decline, Tentative | Performs appointment operations |

URL usage follows this syntax:
http://server_name/virtual_root/folder/?option= Modifier
http://server_name/virtual_root/folder/item_name?Option=&Modifier

For example, the URL entered for *juser* to create a new message might be:
http://owa.microsoft.com/exchange/*juser*/?Cmd=new
Internet Explorer displays the following window when you enter this URL.




Leveraging the basic functions of named URLs can provide fast integration of Exchange with corporate intranet sites.

## WebDAV

Internet Explorer 5 clients support an extension to the HTTP protocol known as WebDAV. WebDAV enables richer manipulation of data on the server over HTTP, thereby allowing the client to work with data in an intuitive manner. WebDAV can accommodate all types of content, so it can be used with many types of documents. You can potentially use WebDAV to author anything you store in a file. WebDAV includes these features:

- *Overwrite protection (file locking).* WebDAV allows users to write, edit, and save shared documents without overwriting another person's work, regardless of which software program or Internet service they use.
- *Namespace management.* Namespace management capabilities permit users to manage Internet files and directories, including allowing them to move and copy files by using a familiar paradigm. The process is similar to the way users manage word-processing files and directories on a local computer.
- *Property (metadata) access.* WebDAV's properties feature is an efficient means of storing and retrieving metadata. Metadata is information about a Web document such as the author's name, the copyright, the

publication date, and keywords that Internet search engines use to find and retrieve relevant documents.

- *Client side rendering:* HTTP-WebDAV offloads the rendering to the client itself by distributing processing and, as a result, increases the capacity of the server.
- *Backward compatibility:* HTTP-WebDAV supports standard methods (GET, POST, PUT, DELTE, OPTIONS), and adds new methods for Web-DAV specific functionality. Because WebDAV is an extenion to HTTP, existing methods are not changed.

❑

More information on WebDAV can be found at http://www.WebDAV.org. WebDAV is defined in RFC 2518.

## Usage Scenarios

Outlook Web Access offers a turnkey solution to many problems facing businesses that are attempting to provide messaging to all areas of an organization. The following sections provide a description of just some of the many usage scenarios that present themselves when armed with the capabilities of Outlook Web Access.

### Light Messaging

Outlook Web Access provides an excellent alternative to the full Outlook 2000 client. There are instances when the use of a full client is either not required or simply not practical, such as when you want to use VPN for messaging access. Outlook Web Access covers these scenarios in an efficient and cost effective manner.

Outlook Web Access is easily applied to the concepts outlined in Zero Administration for Windows. The basic concept is that not every user in an organization requires full messaging functionality. For instance, under the definitions in Zero Administration for Windows, the deployment of Microsoft Office or Outlook 2000 may not be justified for task station and Appstation type computers. Nor would the users of these types of workstations require enhanced messaging functionality.

Knowing the limitations of the Outlook Web Access client will assist in determining which users should be candidates for light messaging. In short, those users who would not normally receive Office 2000 probably do not require Outlook 2000.

The improvements made to Outlook 2000 communication make it more suited to low bandwidth network usage. This makes Outlook Web Access particularly well suited for use over high latency networks. Because of the reduced functionality of the client however, expect the Outlook Web Access client to have much reduced network overhead. For this reason, the implementation of Outlook Web Access makes sense in configurations that cannot spare bandwidth to support the full Outlook client, such as dial-in or Internet-based connections, and demand dial network connections that are serviced “over the wire”.

### Roving User Support

Supporting users that move from computer to computer has always been the nemesis of messaging administrators. Normally, this issue is solved through

system policies and server based profiles that carry a little overhead in terms of administration and performance.
The use of Microsoft Windows® 2000 on the client and back end greatly reduces these burdens and solves issues surrounding roving user support with little administrative effort.
In those instances where it is impractical to implement Microsoft IntelliMirror™ features to solve the problems, you should implement Outlook Web Access. With no client to install other than the browser and no MAPI profile to consider, an Outlook Web Access solution for roving users is indeed an attractive solution. Roving users within the office and over the Internet, as well as home users are well-suited to Outlook Web Access.

### Kiosks

The kiosk scenario places computers in strategic locations such as factory floors, common areas, conference rooms, and so forth, and provides users access to e-mail, calendaring, and other basic messaging functions. This type of solution is particularly attractive for providing general access to posted public folders.

### Migration

Providing functionality to users during a migration continues to be an issue. One of the objectives of migration is to cause as little disruption as possible to normal operations. To accomplish this objective, small groups are migrated at one time, and custom client configurations are deployed to achieve a period of coexistence.
Outlook Web Access is a great solution to the problems that arise from client software coexistence. Although not suitable as a full client replacement, Outlook Web Access is easily deployed and allows users to begin experiencing the power of Exchange as soon as the back end is operational.
When used in conjunction with Internet Explorer 5, the Outlook Web Access interface is so similar to that of the full client, that there should be little learning curve associated with moving between the two clients after deployment is complete.
Migration from other messaging systems to Exchange Server involves deployment considerations not encountered during a more straightforward upgrade. Outlook Web Access again provides a good interim client access solution, which mitigates the operational impact normally associated with extended migration periods.

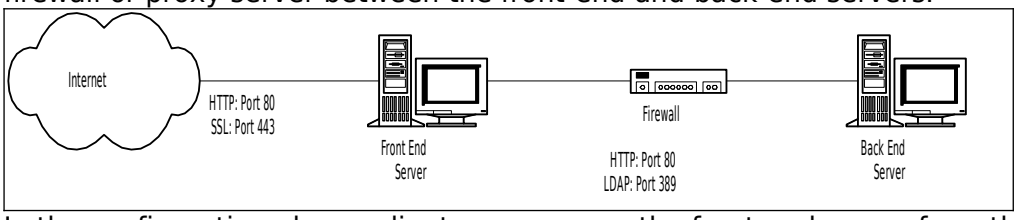
## Planning Considerations

Although Outlook Web Access is operational with very little administrative configuration, there are still strategic points that you must plan before deployment. The two primary items that you must address early on are logical and physical server placement, method of client authentication, and capacity planning.

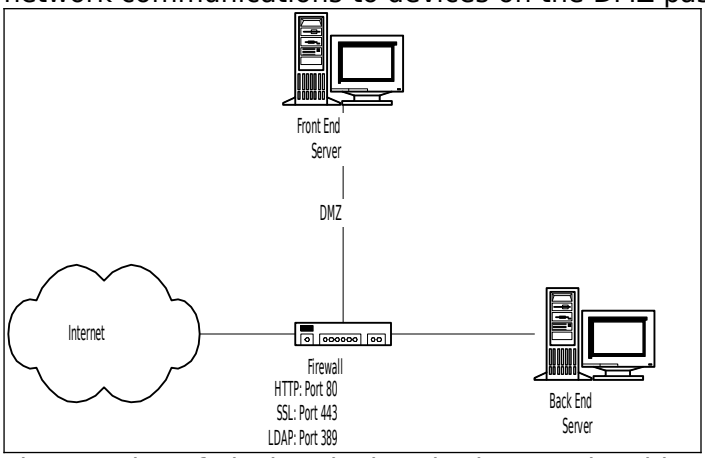
### Network Security

You should pay careful attention to the placement and configuration of Outlook Web Access. You can install Outlook Web Access in either a single or multi-server environment. The decision to deploy Outlook Web Access impacts options available in server placement.

In a multi-server topology, there are several choices for server placement relative to the corporate perimeter network. Back-end servers almost always reside within the corporate WAN. Front-end servers however, can be placed on the perimeter network, the DMZ or internal network depending on the particular circumstance. These scenarios will be covered in order.
The perimeter or exterior network is the network that exists outside (Internet-side) of the firewall or protected internal network. Placement of the front-end server on the perimeter network is a valid occurrence so long as there is a firewall or proxy server between the front-end and back-end servers.

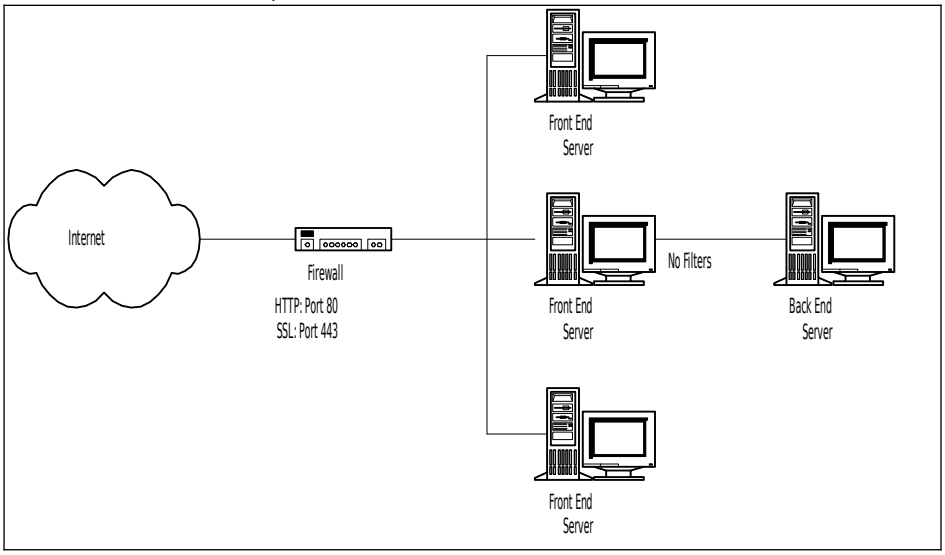



In the configuration above, clients may access the front-end server from the Internet over HTTP and Secure Sockets Layer (SSL). The front-end server in turn authenticates the client to the Active Directory™ directory service (located on the back end in this case) through Lightweight Directory Access Protocol (LDAP) on port 398. Upon the completion of authentication, the front-end server and client communicate by using HTTP or HTTPS, while the front-end and back-end servers communicate over HTTP/HTTPS. Access to the global catalog over TCP/IP port 3268 also may be provided to allow clients to perform password changes.
This configuration is perfectly functional and has practical advantages and disadvantages. The basic configuration ensures that the front-end server is dual-homed to allow port filtering and static mapping independent of the network being addressed. Configuring the front-end server in this manner requires the presence of two network adapters–one on the exterior network and one on the perimeter (exterior to the firewall) network. Static mappings are required to ensure that the front-end server attempts network communications with only the desired Exchange servers. Note that this type of configuration does not protect the front-end server from denial of service attacks.
Placement of the front-end server in the DMZ is another option. The DMZ is an isolated network that sits within the realm of firewall-based communications. All network communications to devices on the DMZ pass through the firewall.




The practice of placing devices in the DMZ has historical significance in a UNIX environment. In the case of Windows 2000 and Exchange 2000 however, this configuration decreases the throughput of the front-end server and restricts the ability to manage the server.

The final configuration for discussion is the placement of the front-end server on the interior network, as illustrated below.




The objective of this configuration is to maximize the use of the front-end servers by allowing both internal and Internet-based clients to access the front-end servers. The other advantage of this configuration is that you can natively manage the front-end servers due to the lack of protocol restrictions on the interior network interface card (NIC).

The front-end servers in this configuration actually exist in two locations and are dual-homed. To prevent direct routing to the interior network, one network interface on the front-end servers is placed on an isolated network that does not route to the interior network. This interface accepts communications from Internet clients. The second interface is bound to the interior network and provides native access.

## Authentication

The default authentication method for Outlook Web Access in a single server environment is Basic and Integrated Windows authentication. In a multi-server environment in which Outlook Web Access is running in a front-end and back-end configuration, the default authentication is set for Basic (clear text) and NTLM protocol. Authentication is set via the HTTP virtual servers configured for Outlook Web Access. Microsoft recommends configuring authentication on the back-end Exchange server only. The default authentication settings are the same on the front-end Exchange server, but securing the back-end server is much more important. In addition, authentication conflicts between the front end and back end could jeopardize user access.

A number of options are available for Outlook Web Access authentication. Choosing the appropriate mechanism is usually a matter of client platform capabilities and specific security policies. Available options for authentication are:

- **Method 1 – Basic**: A simple challenge/response that uses clear text.
- **Method 2 – Integrated Windows**: Leverages the native security attributes of the client.

- **Method 3 – Digest**: Uses effective and efficient cryptology to provide secure authentication.
- **Method 4 – Anonymous**: Cursory authentication used to provide access to public folders that are intended for general access.
- **Method 5 – SSL**: Although not a method, SSL provides a secure communications channel that can be used in combination with any of the above methods.
- The following sections describe Outlook Web Access authentication in more detail.

**Method 1 – Basic**

Basic authentication is a common authentication type on intranets. Unlike NTLM protocol, which accepts established users' identification through the access token, Basic authentication relies on users to enter their user name, domain, and password to authenticate to Outlook Web Access.

**Pros**

Basic authentication is browser independent, making it platform independent.
Basic authentication allows the use of a front-end server.

**Cons**

Basic authentication results in the transmission of unencrypted passwords over the network, making it a relatively insecure method of authentication.
Each time users log on, they must enter their user name, domain, and password.

**Method 2 – Integrated Windows**

Integrated Windows authentication covers a couple of different scenarios. The optimal authentication takes place when the client is operating on Windows 2000 and Internet Explorer 5. This configuration uses Kerberos and offers the best security, efficient communication, and transparency.
When Integrated Windows authentication is used with other non-Windows 2000 Windows networking clients, NTLM protocol is used instead of Kerberos.

**Pros**

Integrated Windows authentication encrypts the client's password and so provides excellent security.
Integration provides native authentication from Windows networking clients.
Kerberos is used when in Internet Explorer 5 on Windows 2000 clients.

**Cons**

Integrated Windows authentication does not work with browsers other than Internet Explorer 4 and 5.
Front-end servers work only when using Internet Explorer 5.
The use of access tokens also increases the overall network traffic.

**Method 3 – Digest**

Digest authentication was introduced about the time that SSL was becoming popular. Digest authentication works by making the client perform a request that is rejected by a security challenge. The challenge specifies that the client is to use Digest and includes a nonce value that the client hashes along with the user name, password and other information. The client hashes the results by using Message Digest 5 (MD5), which is very fast.
The client then re-sends the original message with the hash data. The server re-creates the string on its end, hashes it, and checks the results. If everything matches, then it knows the request is authentic.

**Pros**

Digest authentication works with any HTTP 1.1 compliant browser including Internet Explorer 4.
Digest authentication is fast and secure.

**Cons**

The Exchange front-end or back-end server must be running on a Windows 2000 Domain Controller.

**Method 4 – Anonymous Access**

Anonymous Access allows special use access for specific public folders and directory information.

**Pros**

Anonymous access is supported through all browsers and is an easy way to provide un-secure access to public folder data.
A single point of configuration is used to make administration simple.

**Cons**

Anonymous access does not provide security identity. This prevents tracking usage by user.

Before a user can use Anonymous to access public folders, the root Anonymous public folder must first be published. If anonymous access is not explicitly set, the user is challenged to authenticate.
Select the **Allow anonymous users to access the anonymous public folders** check box.
Make folders visible to Anonymous Outlook Web Access users by clicking them on the **Folder Shortcuts** tab. The selected folder and any subfolders that have anonymous permissions appear.

**Method 5 – Basic over SSL**

SSL provides the best level of security because the entire communications session is encrypted. Although any authentication mechanism can be used with SSL, the most common implementation is with Basic. SSL is not an authentication mechanism itself. Rather, it is used with an authentication mechanism such as Basic to provide a secure channel.

**Pros**

The entire communications session is encrypted.
Most browsers support SSL communication.

**Cons**

SSL requires a substantial amount of session overhead for setup and teardown. Thus, SSL communications reduce the overall performance of the authenticating server.
Like standard Basic authentication, Basic over SSL also displays an **Authentication** dialog box each time the user connects to the server.

**Additional Information on SSL**

The wide spread use of SSL and Transport Layer Security (TLS) encryption with HTTP leads many to believe that they are related. In fact, SSL has absolutely nothing to do with HTTP. SSL is an IP level transport developed to secure TCP/IP protocols such as IMAP, NNTP and HTTP.
The first method of authentication was Basic and had the drawback that it sent the user's password in clear text. SSL however, establishes a secure

communications channel between the client and server, which allows the password to be securely sent. The drawback to SSL is the latency caused by session overhead.

**Front-End and Back-End Authentication**

In Exchange 2000 Beta 3, when using front-end and back-end servers, the front-end server uses the standard IIS authentication to authenticate the client. The front-end server then connects to the back-end server as the user and authenticates to that server as well. This authentication requires that you use authentication and that users have the logon locally right on the front-end server.
Integrated Windows authentication uses Kerberos authentication if supported by the client. To use this type of authentication, clients must use Internet Explorer 5 and Windows 2000.
Specifying Integrated Windows authentication for clients who use software other than Internet Explorer 5 requires NTLM protocol authentication. NTLM protocol authentication does not work with a front-end and back-end topology.

## Capacity Planning

Planning the number of users per Outlook Web Access server is difficult due to the high dependence on client usage behaviors. For example, calendaring requires more server processing than message functions require. Performance of Outlook Web Access in Exchange 2000 is much improved over previous versions, though.
Many organizations tend to use Outlook Web Access as complimentary to full client access. In this case, a prudent figure for planning concurrent Outlook Web Access usage would be about 10 percent of the user population.
Other suggestions for Outlook Web Access planning:
**Usage scenarios:** Will Outlook Web Access be used in a complimentary fashion, in a mixed environment, or will all clients use Outlook Web Access? On the one hand, a limited use Outlook Web Access deployment has fewer concurrent users and thus requires fewer resources. High use Outlook Web Access deployments on the other hand, expand the requirement to a multi server environment that uses separate front-end servers to distribute the client load to several database servers.
Methods used in calculating resource requirements for Outlook Web Access are similar to capacity planning for conventional Exchange deployment. Start with a pilot, and monitor usage and performance impacts.
Many performance counters are exposed to provide data about:

- Logons per day
- Number of messages read
- Number of messages sent
- Session time
- Outlook Web Access connections

Bottlenecks are most likely experienced surrounding IIS sessions. These can be mitigated through load balancing (discussed later).
Also notice that the Outlook Web Access client does not have a button for logging off. To log off of the session, the users must close the browser. Open sessions use server resources, even if the clients are inactive.

**Topology:** The topology affects the number of users served by a particular server.

In a front-end and back-end topology, a front-end server is capable of servicing more than a single back-end server and more than a single front-end server may be used to easily scale to large usage scenarios. The number of front-end servers is also affected by the use of SSL in client communications.
In cases where multiple front-end servers are deployed, reference all servers through a single namespace. Using a single namespace lessens user confusion when adding additional servers. This technique is accomplished by mapping the IP addresses of multiple servers to a single Address record but is not required when using load balancing.

### Load Balancing

When multiple Outlook Web Access servers are being used, you can manually balance their load by assigning groups of users to access a particular server. Compared with other techniques, this has a substantial amount of administrative overhead because the administrator must manually adjust these groupings and monitor the results.
Round Robin Domain Name System (DNS) should not be used to load balance across servers that use SSL due to state information maintained on the server. If redirected to another server by DNS, that state information is lost and the session rebuilt.
The recommendation for load balancing between Outlook Web Access front-end servers is to use Windows Load Balancing available in Windows 2000 or perhaps hardware load balancing, should very high performance be required.
With Windows Load Balancing, all participating server nodes receive client requests. Each Windows Load Balancing Server/Outlook Web Access front end uses a special algorithm based on the IP address of the connecting client to determine if it is the front-end server that should handle the incoming request. If so, it passes the request up the network layer. If not, it discards the request.
Separate NICs are recommended for inter-server communication in a Windows Load Balancing environment. Using this private network, a heartbeat is sent between Windows Load Balancing Server computers so that they can adjust their algorithm for determining which requests to handle if a Windows Load Balancing Server computer comes online or goes offline
Windows Load Balancing Servers are automatically taken out of rotation and others pick up their load, if the heartbeat of one of the computers dies. This provides a degree of fault tolerance for certain types of hardware and software failures.
Resource Kit utilities, such as HTTPMON, and third party tools can be used to monitor like Outlook Web Access. Upon detecting an application failure, you can programmatically take the failing computer out of the Windows Load Balancing Server rotation.

## Installation and Administration

The installation, configuration, and administration of Outlook Web Access is a straight-forward process. Because some of the concepts in Exchange 2000 Outlook Web Access are new, you will want to have a good knowledge of the entire process and the relationships between the components before deployment.

## Setup

Outlook Web Access is installed as part of the default setup of Exchange 2000 and requires Windows 2000 and IIS 5.0 to be installed.
The following table describes the directories relevant to Outlook Web Access installed during Exchange 2000 setup.

| Directory | Contains |
|---|---|
| \exchsrvr\bin | Wmtemplates.dll, which defines the default templates used to render Outlook Web Access. |
| \exchsrvr\exchweb\bin | Exwform.dll, which handles form processing. |
| \exchsrvr\exchweb\ controls | Internet Explorer 5 behavior script and client Microsoft JScript®. This code is separated from the Outlook Web Access ISAPI application for caching by IIS and the client. |
| \exchsrvr\exchweb\lang | Localized versions of Outlook Web Access help files. |
| \exchsrvr\exchweb\img | Graphics used by Outlook Web Access. You can replace the default logo graphics (Owalogo.gif and Owalogoie5.gif) and other graphics in this folder with your own graphics. Any modifications made are lost during and upgrade of the Exchange 2000 software. |

Four virtual IIS directories are created by Setup and are exclusive to Outlook Web Access.

| Web Virtual Directory | Function |
|---|---|
| /exchweb | Stores graphics and other ancillary files by Outlook Web Access. |
| /exadmin | Is used by the Exchange Administration tool to administrate public folders. |
| /exchange | Stores the mailbox root. |
| /public | Contains the default public folders tree. |

## Server Configuration

Outlook Web Access is configured by default to allow access to users' mailboxes and the default public folder tree. However, you can configure the server to provide customized access for HTTP/WebDAV clients. You can specify items such as:

- Which users can access the server from a Web browser.
- Which authentication method(s) to allow.
- Which public folders are exposed to users.

To perform this configuration, you use the Exchange System Manager console and the Active Directory Users and Computers console in the Microsoft Management Console (MMC). The changes you make are stored in the Active Directory and then applied by the appropriate Exchange server.

**Note:** The virtual Web servers and directories that you create with the Exchange Administration tool also appear in the Internet Services Manager console. Configuration changes made in the Exchange Administration tool overwrite changes made to similar items with Internet Services Manager. Use only Internet Services Manager to make changes to items that are not available in the Exchange Administration tool.

## Outlook Web Access User management

Web access to Exchange 2000 is enabled for all users by default. To enable or disable this value you must use Active Directory Users and Computers. When View Advanced Features is enabled, you can see the Exchange **Advanced** tab in the user properties. On this tab is the **Protocols Settings** button, which allows you to modify the HTTP, POP3 and IMAP4 access settings for the user.

## Virtual Servers and Directories

Virtual servers allow you to create separate Web server instances for internal and external users for different departments within a company or for users with different security requirements.
When creating an HTTP virtual server there are three areas of configuration:

- General. This configures the virtual server identification (host header, IP address, port), number of connections available to content (private mailboxes or a specific portion of the public folder tree), and logging.

**Note:** The combination of identification values for each virtual server must be unique.

- Access. This configures whether anonymous access is allowed to content shared by the virtual server and which type of the authentication methods to allow for secured content.
- Security. This configures administrator permissions to the virtual server and does not affect client connections.

❑

#### Connecting to a Virtual Server

A browser connects to a specific virtual server by specifying http://*IP Address:Port* or http://*host header name:Port*. The port does not need to be specified if it is the default TCP port 80. The host header name should be registered as a host record in DNS, or added to the client's host file, or match the server's computer name if the connection occurs on an intranet.
When the server receives the request, it looks at the server name in the URL to determine which virtual server receives the request. If the server name specified matches the host header of a virtual server, it directs the request to that server. Otherwise default Web Server handles the request.

#### Disabling Virtual Servers

Exchange Server 5.5 Outlook Web Access allowed you to enable or disable all HTTP access for Exchange on the **General** tab. Exchange 2000 has similar functionality. You can now stop, start, or pause each virtual server by right-clicking the virtual server object in the administration tool and clicking the appropriate option.

**Note:** If you stop the default Exchange Virtual Server, you are stopping the IIS Default Web Server. If you want this Web server to be available but eliminate Exchange access, you can remove the Exchange, Exadmin, and public virtual directories. You can also configure security to disable access. Removing virtual directories effectively disables management of public folders on the subject server.

For each virtual server, you can configure multiple virtual directories to point to different public folders or to the private mailbox store[2]. In Beta 3, virtual directories can be created within other virtual directories allowing you to create your own Web accessible hierarchy. This hierarchy can then be traversed through Web folders or used by your Web applications.
Virtual directories are similar to the public folder shortcuts used in previous version of Exchange.

#### Front-End Servers

To configure a front-end server in Exchange 2000 beta 3, you must select the **This is a front end server** check box in the server's **Properties** dialog box, and then restart the Exchange and IIS services or restart the computer.
By making this change, you are instructing the HTTP, POP3, and IMAP4 components of Exchange to proxy all traffic to a back-end server that contains the user's mailbox. The Information Store remains intact on the server and is available to MAPI clients, however it is not accessed by these three protocols.
It is recommended for front-end servers that you configure it immediately after install as a front-end server and then disable the Exchange Information Store service.

## Multilanguage Support

Exchange 2000 will be localized into 6 languages: English, French, German, Japanese, Italian, and Spanish. Outlook 2000 will support the same 22 client languages supported in Outlook Web Access 5.5. Exchange 2000 will support all Outlook languages through installed locales.

### Configuring Multilanguage support

Language support in Outlook 2000 stems from the configuration of Locales within Exchange 2000 itself. To configure multi-language support for Outlook Web Access:

- Select the desired languages from the **Advanced** tab of the **Server Properties** dialog box in Exchange System Manager.
- Install localized Outlook Web Access templates from the self extracting template located on the server CD.

[2] Each virtual server created should have a corresponding DNS alias configured to provide named access to the virtual server.

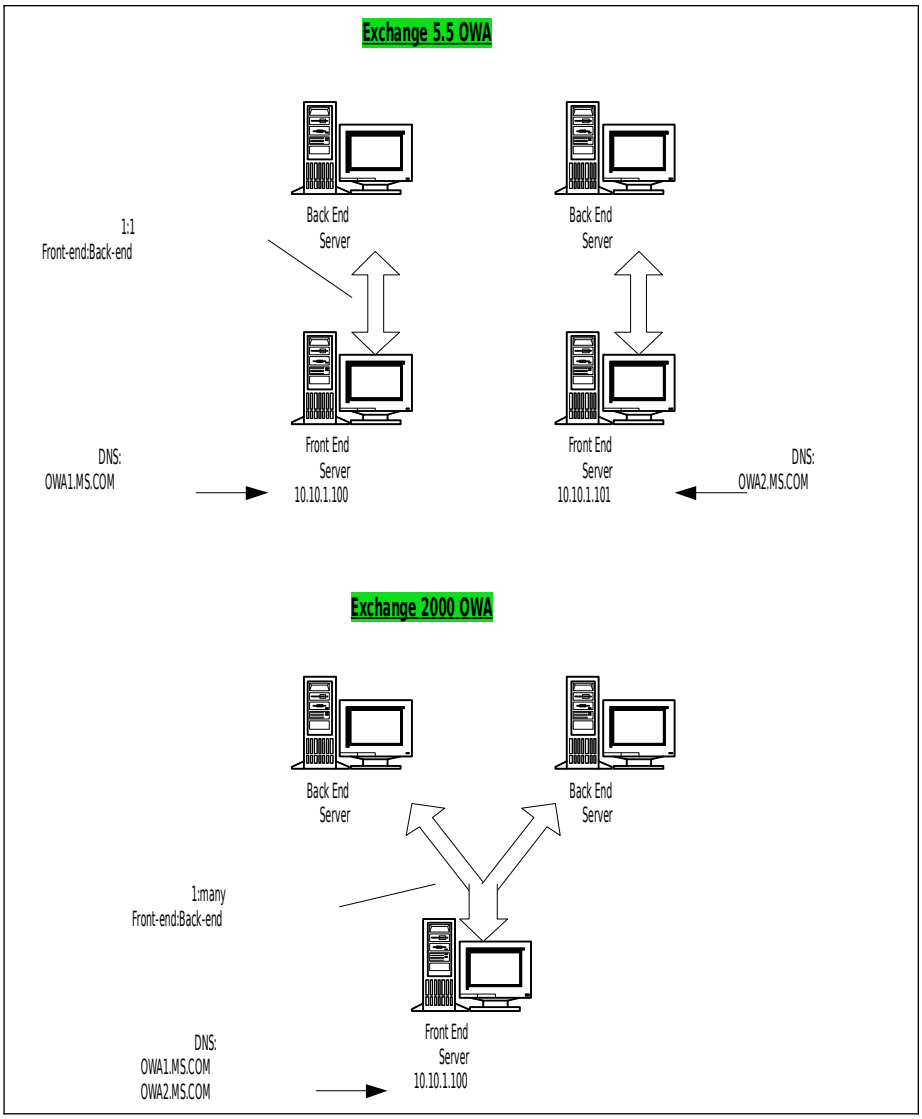
- Ensure that proper locale is installed on server.

## Migration Issues

There are a few issues associated with transitioning from Exchange 5.5 Outlook Web Access to Exchange 2000 Outlook Web Access. If the installation or migration of Outlook Web Access is simultaneous, the upgrade consists of replacing services and updating DNS to reflect the new Outlook Web Access servers. If you’re performing the upgrade on a stand-alone server, you do not need to make adjustments to DNS.

Often Exchange 5.5 Outlook Web Access front-end servers must be maintained for a period during the migration process. This may be required to support customizations or CDO based Web applications, but with Outlook Web Access that have been done on the legacy system they will not be supported on the new Outlook Web Access servers.

Exchange 5.5 Outlook Web Access front end may be used against an Exchange 2000 Outlook Web Access back end. The primary consideration is the eventual integration of the front-end servers with Exchange 2000 Outlook Web Access. Due to the increased performance of Exchange 2000, there will likely be fewer Exchange 2000 front-end servers after the transition is complete. Unless the Exchange 5.5 Outlook Web Access is being used in conjunction with Windows or hardware load balancing, the DNS entries that were servicing multiple legacy front-end servers will be directed to a single device.




Likewise, more than a single URL may be used to address the same front-end server. This will help minimize the user confusion associated with changing the virtual server name during migration.

Alternatively, establish the new Exchange 2000 Outlook Web Access servers parallel to the legacy servers, and simply define new URLs, or move the entire system at a specified date.